Formación de Auditores Internos ISO27001 y Técnicas de Hacking ético

Ruiz Gómez Julio Cesar
julioc_rg_@hotmail.com
Especialización en Seguridad Informática
Universidad Piloto de Colombia.

Abstract—In this document an introduction to the principles in the formation of internal Auditors in ISO27001 will be given, explaining some basic concepts about information security, some basic definitions associated with security, important aspects in the audit process, how to build an audit plan and how to carry out the audit process.

Some ethical hacking techniques will be described, where we will have some general concepts, how to perform the discovery, enumeration, vulnerability analysis and how would be the exploitation of these.

Resumen—En este documento se dará una introducción en los principios en la formación de Auditores internos en la norma ISO27001, explicando algunos conceptos básicos sobre seguridad de la información, algunas definiciones básicas asociadas con la seguridad, aspectos importantes en el proceso de auditoría, como construir un plan de auditoria y como llevar a cabo el proceso de auditoría.

Adicionalmente se describirá algunas técnicas de hacking ético, en donde tendremos algunos conceptos generales, como realizar el descubrimiento, enumeración, análisis de vulnerabilidades y como sería la explotación de estas.

Indice de Términos—*Auditoria, Auditores, ético, explotación, hacking, seguridad, vulnerabilidades.*

I. INTRODUCCIÓN

Las Auditorias existen con el objetivo de evaluar el cumplimiento de las políticas que tiene la empresa y si están bien planteados para el cumplimiento de su objetivo general evaluando que los procedimientos que llevan a cabo son los adecuados; Para este caso se tendrán en cuenta las normas de seguridad basadas en la Norma ISO27001:2013.

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento de la persona, empresa o sistema [1].

La informática es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores [2].

La seguridad es el conjunto de medidas y acciones que se aceptan para proteger un ente contra determinados riesgos a que se está expuesto.

Las infraestructuras críticas Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor a la población [3].

El hacking ético se describiría como la defensa contras las amenazas constantes en el ciber espacio brindando la posibilidad de controlarlas, erradicándolas, buscando de donde provienen, quien la puede estar ejecutando. Algunos conceptos enfocados en la seguridad de los sistemas.

La amenaza es la acción o evento que puede afectar la seguridad.

La vulnerabilidad es la debilidad que puede ocasionar un comportamiento no esperado que afecta la seguridad de los sistemas.

Los exploit son el camino definido para vulnerar la seguridad de un sistema de TI utilizando una vulnerabilidad [4].

Un ataque se define como cualquier acción que viola la seguridad [4].

II. SEGURIDAD

Conjunto de medidas y acciones que se aceptan para proteger un ente contra determinados riesgos a que se está expuesto.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema [5].

Un sistema informático puede ser protegido desde un punto de vista lógico o físico.

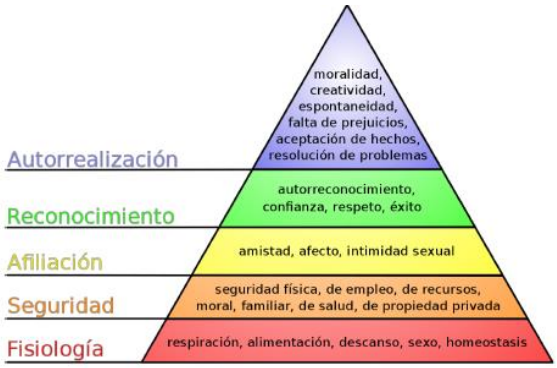

Fig. 1 Pirámide de Maslow, jerarquía de las necesidades humanas, obtenida de https://www.leyatraccionpositiva.com/piramide-maslow-psicologia/

A. Tipos de seguridad en sistemas

- Seguridad Física (Seguridad de la Información): Son todos aquellos mecanismos generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

  Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta [6].

  Problemas a los que nos enfrentamos:
  - Acceso físico
  - Desastres naturales
  - Alteraciones del entorno
- Seguridad lógica (Seguridad Informática): Es una referencia a la protección por el uso de software en una organización, e incluye identificación de usuarios y contraseñas de acceso, autenticación, derechos de acceso y niveles de autoridad [7].

  La seguridad lógica incluye entre otros lo siguiente:
  - Los virus
  - Programas no testeados
  - Errores de usuario
  - Error del operador
  - Mal uso del ordenador
  - Fraude informático
  - Investigación de accesos no autorizados internos
  - Acceso no autorizados externos

Fig. 2 Seguridad de la información e Informática, obtenida de la presentación Formación Auditores 27001 material de trabajo del Seminario de Investigación Aplicada en Gestión de la Seguridad y el Riesgo

B. Pilares de la seguridad

Estos se conforman por la integridad, disponibilidad y confidencialidad en donde se tiene otras propiedades como la autenticidad y el no repudio de la información.

Fig 3. Pilares de la seguridad informática, obtenida de la presentación Formación Auditores 27001 material de trabajo del Seminario de Investigación Aplicada en Gestión de la Seguridad y el Riesgo

C. Conceptos adicionales

El no repudio se define como evitar rechazar la autoría de una comunicación o de un documento. cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

- La autenticidad: Es la propiedad de una entidad es lo que afirma ser.
- La responsabilidad (Accountability): Se refiere a que toda operación realizada en el sistema de información lleve asociada la información de quién la ejecutó, cuándo, y desde donde.

Permitiendo determinar quién hizo qué en el sistema con los recursos, de manera que se pueda establecer quién es el responsable de todas y cada una de las operaciones ejecutadas.

- La auditabilidad**:** Consiste en que se pueda revisar lo que las personas hacen con el sistema y validar que se haga dentro de parámetros adecuados de operación y de acuerdo a la normatividad interna de la organización y la legislación vigente.

Que exista auditabilidad el sistema debe generar trazas de auditoria que permitan reconstruir lo que un usuario ha hecho en/con el sistema, y estas deben mantenerse íntegras y seguras, fuera del alcance de todas las personas.

- La Amenaza: Se describe como cualquier agente capaz de aprovechar una falla del sistema de gestión de seguridad de la información, con la finalidad de causar perdida o destrucción de la información o de sus recursos tecnológicos, en pocas palabras, de los ac6vos de información de la organización.
- La vulnerabilidad: Es una debilidad en un sistema, el cual permite enfocar la integridad, disponibilidad, confidencialidad de la información.
- El riesgo: Probabilidad de ocurrencia de un hecho (amenaza), es decir, posibilidad de que se exploten vulnerabilidades, causando pérdidas o daños a los activos de información e impactando profundamente los objetivos de la organización.
- Los controles**:** Son el Conjunto de medidas establecidas por la organización para lograr mitigar o erradicar la probabilidad de existencia de los riesgos que afecten los activos de información de la organización [2].

III. AUDITORIA

Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas objetivamente a fin de determinar hasta qué punto los criterios se cumplen [2].

Considerada como el examen y control de la situación económica de la empresa, para saber qué cosas van mal, qué cosas van bien y cómo se puede mejorar en cualquiera de los puntos clave de la empresa. Auditar, se entiende así, como someter las cuentas de una empresa a examen para saber cómo está actualmente la empresa para saber hacia dónde debe ir a partir de ese momento [8].

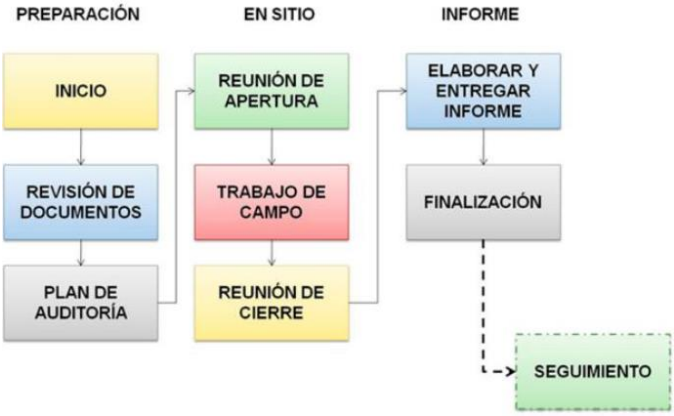

Fig. 4 Ciclo de ejecución de una Auditoria, obtenida de la presentación Formación Auditores 27001 material de trabajo del Seminario de Investigación Aplicada en Gestión de la Seguridad y el Riesgo

A. *Modalidades de la auditoría*

Se clasifican en tres las cuales son regular, especial y de seguimiento.

- Regular: Se aplica por decisión interna o externa, para propósito de certificación, emitir conceptos sobre la gestión.
- Especial: Cuando existe un interés especial en examinar uno o varios procesos del sujeto o punto de control.
- Seguimiento: Se aplica sobre planes de mejora o planes de acción surgidos de manera propia o a partir de otras auditorías.

B. *Conceptos claves de la auditoria*

- Criterios de Auditoría: Conjunto de políticas, procedimientos o requisitos utilizados como referencia.
- Evidencia de la Auditoría: Registros, declaraciones de hecho u otra información que son relevantes para los criterios de auditoría.
- Hallazgos de la Auditoría: Resultados de la evaluación de las evidencias de la auditoría, frente a los criterios de la auditoría. Pueden indicar la conformidad y no conformidad con los criterios de auditoría u oportunidades para la mejora.

C. *Participantes de la auditoria*

El equipo auditor está conformado por el líder auditor, el equipo auditor conformado por el Auditor en formación, Auditor, Auditor experto y el observador.

Fig. 5 Equipo Auditor, obtenida de la presentación Formación Auditores 27001 material de trabajo del Seminario de Investigación Aplicada en Gestión de la Seguridad y el Riesgo

D. *Preliminares*

Programa de Auditoría: Conjunto de una o más auditorías planificadas para un periodo de tiempo específico.

Plan de Auditoría: Descripción de las actividades y preparativos de una auditoría.

Alcance de la Auditoría: Extensión y límites de una auditoría.

Competencia: Capacidad de mostrada para aplicar conocimientos y habilidades [2].

IV. HACKING ÉTICO

Acto de una persona que usa sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

A. *Rol del hacker ético*

Se puede asimilar al papel de un auditor en donde evalúa el estado de la seguridad de un sistema o infraestructura tecnológica, analizar los resultados obtenidos de la auditoría técnica, reporta asertivamente los hallazgos a las partes interesadas y desempeña el papel de experto en un equipo auditor.

B. *Términología*

- Análisis de Vulnerabilidad: Análisis de sistemas informáticos en búsqueda de vulnerabilidades conocidas, con el fin de listar las y clasificarlas de acuerdo a su criticidad (alto, medio, bajo). No es característico de un análisis de vulnerabilidad explotar las vulnerabilidades encontradas.
- PenTest (Penetration Test): Ejecución controlada de "exploits" de vulnerabilidades encontradas en un análisis de vulnerabilidad previo.

V. PRUEBAS DE PENETRACIÓN

Se realizan desde la posición de un atacante potencial de manera remota y local. A través de técnicas de Hackeo Ético se busca explotar activamente las vulnerabilidades de seguridad para obtener información relevante. Tal como lo intentaría un intruso con propósitos adversos para la

organización. En conjunto con el cliente diseñamos y ejecutamos escenarios reales que permitirán identificar áreas de oportunidad para disminuir el impacto y la probabilidad de ciberataques.

Por qué realizar Pruebas de Penetración:

1) Conocer su madurez en Seguridad Informática: Organizaciones que requieren conocer de forma amplia y profunda la efectividad de sus controles y el estado actual de su seguridad en Tecnologías de Información.

2) Cumplimiento Regulatorio: Instituciones que necesitan cumplir con regulaciones como LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de Particulares), ISO/IEC 27001, PCI-DSS, etc., y requieren realizar pruebas de penetración de forma periódica.

3) Mejores Prácticas: Más allá del cumplimiento regulatorio, muchos marcos de trabajo globalmente aceptados como ISO, COBIT, etc. recomiendan la ejecución de pruebas de penetración como parte de una gestión de seguridad proactiva.

4) Obligaciones Contractuales: Muchas organizaciones requieren hacer pruebas de penetración como parte de obligaciones contractuales con socios o clientes [9].

A. Clasificación de pruebas de penetración

1) Se clasifican por el origen de las pruebas internas y externas:

- Pruebas de penetración externas: Se realizan desde lugares externos a las instalaciones de la organización. Se evalúan mecanismos perimetrales de seguridad informática.
- Pruebas de penetración internas: Se realizan dentro de las instalaciones de la organización para evaluar las políticas y mecanismos internos de seguridad de la organización [10].

2) Por el conocimiento de los objetivos este tipo de pruebas que se realizan son de caja negra, caja gris y caja blanca:

- Pruebas de caja negra: Las pruebas de caja negra implican la realización de una evaluación de la seguridad y pruebas sin conocimiento previo de la infraestructura o de la infraestructura de red a probar. La prueba simula un ataque de un hacker malicioso fuera del perímetro de seguridad de la organización.
- Pruebas de caja blanca: Las pruebas de caja blanca implican la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura de red, como un administrador de red podría hacer.
- Pruebas de caja gris: Las pruebas de caja gris implican la realización de la evaluación de la seguridad y pruebas internas. Las pruebas examinan el grado de acceso a información privilegiada dentro de la red. El propósito de esta prueba es para simular las formas más comunes de ataque, los que se inician desde dentro de la red. La idea es poner a prueba o auditar el nivel de acceso de los empleados, o contratistas y ver si esos privilegios se pueden escalar a un nivel superior [11].

B. Triángulo de la Seguridad, funcionalidad y facilidad de uso

Como profesional de la seguridad, es difícil encontrar un equilibrio entre la instauración de barreras de seguridad para evitar un ataque y permitir que el sistema permanezca funcional para los usuarios. El triángulo de la seguridad, funcionalidad y facilidad es una representación del equilibrio entre la seguridad, la funcionalidad y la facilidad de uso para los usuarios del sistema. En general, cuando la seguridad aumenta, la funcionalidad y facilidad de uso para los usuarios del sistema disminuye.

Fig. 6 Triangulo de la Seguridad, obtenida de http://ehack.info/tipos-de-pruebas-de-penetracion/

En un mundo ideal, los profesionales de la seguridad les gustaría tener el más alto nivel de seguridad en todos los sistemas; Sin embargo, a veces esto no es posible. Demasiadas barreras de seguridad dificultan el uso de los sistemas a los usuarios e impiden la funcionalidad del sistema.

C. Investigación de vulnerabilidades y herramientas

El estudio de vulnerabilidades es el proceso de descubrimiento de vulnerabilidades y debilidades de diseño que podría conducir a un ataque a un sistema. Existen varios sitios web y herramientas para ayudar a los hackers éticos en el mantenimiento de una lista actualizada de vulnerabilidades y posibles agujeros de seguridad de los sistemas o redes. Es esencial que los administradores de sistemas se mantengan actualizados sobre los últimos virus, Troyanos y otros ataques comunes a fin de proteger adecuadamente sus sistemas y redes. Además, al familiarizarse con las nuevas amenazas, un administrador puede aprender a detectar, prevenir y recuperarse de un ataque.

D. Realización de una prueba de penetración

Muchos hackers éticos que desempeñan el papel de profesionales de seguridad utilizan sus habilidades para llevar a cabo evaluaciones de seguridad o pruebas de penetración. Estas pruebas y evaluaciones tienen tres fases, generalmente ordenadas de la siguiente manera:

1) Preparación: Esta fase consiste en un acuerdo formal entre el hacker ético y la organización. Este acuerdo debe incluir el alcance completo de la prueba, los tipos de ataques (Internos o externos) a utilizar, y los tipos de pruebas: caja blanca, negra o gris.

2) Realizar evaluación de la seguridad: Durante esta fase, las pruebas se llevan a cabo, después de lo cual el pentester prepara un informe formal de vulnerabilidades y otros hallazgos [11].

VI. INFORME DE HACKING ÉTICO

El resultado de una prueba de penetración en una red o una auditoría de seguridad es un informe de hacking ético, o de pen test. Cualquier nombre es aceptable, y se puede utilizar indistintamente. Este informe detalla los resultados de la actividad de hackeo, los tipos de pruebas realizadas y los métodos de hacking usados. Los resultados se comparan con las expectativas inicialmente acordadas con el cliente.

A. Presentación de reportes

La presentación de los resultados debe ser de manera asertiva, ordenada, clara, completa todo esto considerando el perfil, conocimiento e interés del lector.

B. Reportes técnicos

Dirigidos a grupos encargados de la remediación a líderes, técnicos del Proyecto, analistas de TI o de Seguridad, etc.

Compilado del detalle técnico – deben ser exhaustivos.

Son una Herramienta para toma de decisiones de tipo técnico.

El contenido de este reporte debe contener una Introducción, objetivos, alcance, metodología, resultados, conclusiones, recomendaciones y anexos.

C. Reportes ejecutivos

Presentación Resumida de Resultados Relevantes dirigidos a gerentes y directores.

Se debe minimizar el uso del lenguaje técnico especializado.

Debe ser comprensible para un lector sin conocimientos en el tema.

El contenido de este reporte debe contener una Introducción, objetivos, alcance, metodología, resultados, conclusiones y recomendaciones [4].

VII. COMO SER ÉTICO

El hacking ético se suele llevar a cabo de una manera estructurada y organizada, por lo general como parte de una prueba de penetración o de auditoría de seguridad. La profundidad y amplitud de los sistemas y aplicaciones a verificar se fija normalmente a partir de las necesidades y preocupaciones del cliente. Muchos hackers éticos son miembros de un equipo tigre. Un equipo tigre trabaja en conjunto para realizar una prueba a gran escala que cubre todos los aspectos de la red, físico e intrusión en los sistemas.

Los pasos siguientes son un marco para la realización de una auditoría de seguridad en una organización y ayudará a asegurar que la prueba se lleva a cabo de una manera organizada, eficiente y de manera ética:

- Hablar con el cliente, y discutir las necesidades a ser consideradas durante la prueba.
- Preparar y firmar documentos de confidencialidad también conocidos como (DNA) con el cliente.
- Organizar un equipo de hacking ético, y preparar un calendario para la prueba.
- Llevar a cabo la prueba.
- Analizar los resultados de las pruebas, y preparar un informe.
- Presentar los resultados del informe al cliente.

VIII. CONCLUSIONES

Actualmente todas las empresas requieren de asesoría para el cumplimiento de sus objetivos y aquí es donde los Auditores tienen su papel validando los controles de seguridad que maneja la empresa en donde validan el cumplimiento por parte de todos los empleados de la organización incluyendo los gerentes y ejecutivos, si son suficientes o si se requiere de otros, mejorando así la protección de lo más importante para la empresa que son los activos de información.

Se permitió conocer más sobre la seguridad, los pilares la importancia de esta y a que riesgos se puede estar expuesto; Adicional a esto se amplió el conocimiento en cómo se realiza una Auditoria aclarando que se debe pedir en primer lugar al cliente y que documentos se presentan al final al cliente y quienes conforman el equipo auditor. Se amplió el conocimiento en conceptos de hacking ético, el rol que desempeña la persona que realiza esta actividad, los pasos que se desarrollan para el tratamiento de vulnerabilidades desde su hallazgo hasta su control o posible eliminación y finalmente los tipos de reporte que se pueden presentar dependiendo de la persona si es técnica o a un gerente y de su conocimiento.

AGRADECIMIENTOS

Se agradece a todos los ingenieros que nos instruyeron en el seminario de investigación aplicada en gestión de la seguridad y el riesgo de la Universidad Piloto de Colombia en donde nos compartieron sus experiencias en el campo profesional y asignándonos actividades cuyo objetivo era simular una experiencia de la vida real y aplicarle una solución con lo visto en el seminario.

REFERENCIAS

[1] TIC's (tecnologías de la información y comunicación). [Online]. Disponible: https://www.mindmeister.com/es/594648644/tic-s-tecnologias-de-la-informacion-y-comunicacion.

[2] D. L. Toro Betancur, Presentación Formación Auditores 27001, Bogotá, Colombia, 2018.

[3] R. Quevedo, Presentación Hacking Ético, Bogotá, Colombia, 2018.

[4] Glosario de Informática e Internet. [Online]. Disponible: https://www.internetglosario.com/1131/hackingetico.html

[5]Definición.DE, "Definición seguridad". [Online] Disponible: https://definicion.de/seguridad-informatica/
[6] Leyatraccionpositiva," Seguridad Física". [Online] Disponible: https://www.leyatraccionpositiva.com/piramide-maslow-psicologia/
[7] universidadviu," Seguridad lógica". [Online] Disponible: https://www.universidadviu.com/conceptos-seguridad-logica-informatica/
[8] Emprendepyme," Auditoria". [Online] Disponible: https://www.emprendepyme.net/auditoria
[9] Protektnet," Pruebas de penetración". [Online] Disponible: https://protektnet.com/servicios/analisis-de-seguridad/pruebas-de-penetracion/
[10] tecnoxxi," Pruebas internas y externas". [Online] Disponible: https://www.tecnoxxi.com/blog/seguridad-informatica/que-es-ethical-hacking/
[11] ehack," Pruebas de penetración". [Online] Disponible: http://ehack.info/tipos-de-pruebas-de-penetracion/

Autor

Julio Cesar Ruiz Gómez, Ingeniero de Sistemas de la universidad Unipanamericana Compensar título obtenido en junio del 2014 y actualmente culminando estudios de la especialización en Seguridad Informática de la Universidad Piloto de Colombia.